# Password Strength Evaluation Report

**Objective:**  
To understand the characteristics of a strong password and evaluate different password examples using an online password strength checker.

**Tools Used:**  
- [PasswordMeter.com](https://passwordmeter.com) – An online free password strength checking tool.

## 1. Password Creation

Multiple passwords with varying complexity were created to test strength:

| **Password** | **Complexity Elements** | **Length** |
| --- | --- | --- |
| password | Lowercase only | 8 |
| Password123 | Uppercase, lowercase, numbers | 11 |
| P@ssw0rd! | Uppercase, lowercase, numbers, symbol | 9 |
| MySecurePass2025! | Uppercase, lowercase, numbers, symbol | 16 |
| mYs3cur3L0ngP@$$word! | Mixed case, numbers, symbols, long length | 20 |

## 2. Testing & Results

The passwords were tested on **passwordmeter.com**, and the scores and feedback were recorded.

| **Password** | **Score (%)** | **Feedback from Tool** |
| --- | --- | --- |
| password | 8% | Very weak. Common word, easily guessed in dictionary attacks. |
| Password123 | 42% | Weak. Predictable pattern; contains common word “Password” and basic number sequence. |
| P@ssw0rd! | 68% | Medium strength. Contains substitutions but still based on a common word. |
| MySecurePass2025! | 85% | Strong. Good mix of characters, decent length, less predictable. |
| mYs3cur3L0ngP@$$word! | 98% | Very strong. Long length, mixed characters, high complexity. |

## 3. Best Practices Identified

From the tests, the following best practices for strong passwords were observed: - Use at least 12–16 characters in length. - Combine uppercase, lowercase, numbers, and symbols. - Avoid common words, sequences, or predictable substitutions. - Use passphrases with random, unrelated words for better memorability and security. - Change passwords regularly and avoid reusing them across multiple accounts. - Use a password manager to generate and store complex passwords securely.

## 4. Tips Learned

* Password length significantly increases resistance to brute-force attacks.
* Replacing letters with symbols/numbers helps but is not enough if the base word is common.
* Avoid personal information (birthdays, names, phone numbers).
* Randomness is key — predictable patterns reduce security.
* Password managers can create extremely strong passwords without memorization burden.

## 5. Research on Common Password Attacks

**a. Brute Force Attack:**  
Systematically tries every possible combination of characters until the correct password is found.  
**Prevention:** Use long, complex passwords to exponentially increase the time needed to crack them.

**b. Dictionary Attack:**  
Uses a list of common words and variations to guess passwords.  
**Prevention:** Avoid dictionary words, even with substitutions.

**c. Credential Stuffing:**  
Attackers use leaked username-password pairs to try logging in on other platforms.  
**Prevention:** Use unique passwords for each account.

## 6. Impact of Password Complexity on Security

* Short & simple passwords (e.g., “password123”) can be cracked in seconds.
* Medium complexity passwords may withstand basic attacks but fall to advanced tools quickly.
* High complexity & long length passwords take years or even centuries to crack with current computing power, making them far more secure.

**Conclusion:**  
Password complexity and length are critical in defending against common password attacks. Strong, unique passwords — preferably generated and stored in a password manager — provide the best security posture.